UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,246	04/30/2001	Yves Louis Gabriel Audebert	741.01101	8917

7590 08/22/2008

STEVENS, DAVIS, MILLER & MOSHER, LLP
1615 L Street, N.W., Suite 850
Washington, DC 20036

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
08/22/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/844,246	AUDEBERT ET AL.	
	Examiner	Art Unit	
	BENJAMIN E. LANIER	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9,10 and 15-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9,10,15-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

2. Claim 1 is objected to because of the following informalities: Claim 1 recites, "a first client data processing receiving…" and "a second client data processing receiving…" Previous amendments removed "means for" language, which leaves simply "client data processing". This is believed to be a typographical error. Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. Claims 1-7, 9, 10, 15-17, 19-39, 41, 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over DiGiorgio, U.S. Patent No. 6,385,729, in view of Graham, U.S. Patent No.

6,402,028, and further in view of Elgamal, U.S. Patent No. 5,657,390. Referring to claims 1, 42, DiGiorgio discloses a secure token device access system wherein a secure token device and a local computer system communicate via a token reader, and by passing data packages known as application protocol data units (APDUs) using the reader (Col. 1, line 63 – Col. 2, line 13 & Col. 9, lines 1-6), which meets the limitation of client communications means for transmitting and receiving message packets over said network using a packet based communications protocol, and for transmitting and receiving APDUs through said PSD interface. When a user attempts to access ISP services from the token device, the ISP issues a challenge to the token device to ensure that the user should be granted access to the ISP services (Col. 2, lines 16-23 & Col. 10, lines 24-33), which meets the limitation of a first client data processing means for receiving incoming message packets from said remote computer system using said client communications means. Once the challenge is received at the token device, the token device issues a response to the ISP challenge in the form shown in Figure 8B (Col. 10, lines 33-35), which meets the limitation of second client data processing means for receiving incoming APDUs from said PSD interface. DiGiorgio does not specify that the ISP services provide command instructions to the secure token device and visa versa. Graham discloses a system wherein smart cards and remote servers communicate through a host terminal by passing network packets from the smart card and the server that contain smart card commands instructions (i.e. APDUs) (Col. 22, line 51-Col. 23, line 20), which meets the limitation of separating APDUs from said incoming message packets thus generating APDUs and routing said APDUs to said PSD through said PSD Interface independently of the origin and integrity of said incoming message packets, incoming APDUs into outgoing message packets and routing said outgoing message packets to said remote

computer system through said client communications means. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the secure token access system of DiGiorgio to provide network communication between the secure token device and the ISP server in the manner discussed in the Graham in order to provide multi-application secure token devices that are customizable and allow for unique variations of applications to be loaded onto the individual card post-issuance as taught by Graham (Col. 5, lines 7-18). DiGiorgio discloses that the local computer communicates with the remote computer using a web browser (Abstract) over the network. DiGiorgio does not disclose that the packets transmitted between the local computer and remote computer are encapsulated. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to encapsulate the packets transmitted from the local computer to the remote computer in DiGiorgio using SSL in order to provide a security in communications over networks that is platform independent, that can work with many different types of applications that request a wide variety of different types of server applications, and which can be performed with minimal time and effort as taught by Elgamal (Col. 1, lines 11-19, 39-55).

Referring to claim 2, DiGiorgio discloses a secure token device access system wherein a secure token device and a local computer system communicate via a token reader, and by passing data packages known as application protocol data units (APDUs) using the reader (Col. 1, line 63 – Col. 2, line 13 & Col. 9, lines 1-6), which meets the limitation of at least one PSD comprising means for functionally connecting to said PSD interface and mans for functionally communicating through said interface, PSD communications means for transmitting and receiving APDU messages through said PSD interface. When a user attempts to access ISP

services from the token device, the ISP issues a challenge to the token device to ensure that the user should be granted access to the ISP services (Col. 2, lines 16-23 & Col. 10, lines 24-33), which meets the limitation of PSD processing means for interpreting said APDU messages, executing commands included in said APDU messages. Once the challenge is received at the token device, the token device issues a response to the ISP challenge in the form shown in Figure 8B (Col. 10, lines 33-35), which meets the limitation of transmitting responses in APDU format through said PSD interface using said communications means. The secure token device contains a unique ID that is encoded into the token device (Col. 10, lines 54-55), which meets the limitation of memory storage means for storing at least one unique identifier.

Referring to claim 3, DiGiorgio discloses that when a user attempts to access ISP services from the token device, the ISP issues a challenge to the token device to ensure that the user should be granted access to the ISP services (Col. 2, lines 16-23 & Col. 10, lines 24-33), which meets the limitation of server communications means for transmitting and receiving messages over said network using said packet based communications protocol, first server data processing means for receiving requests from at least one applications level program,. Once the challenge is received at the token device, the token device issues a response to the ISP challenge in the form shown in Figure 8B (Col. 10, lines 33-35), which meets the limitation of third server data processing means for receiving incoming messages from said local client using said server communications means. DiGiorgio does not specify that the ISP services provide command instructions to the secure token device and visa versa. Graham discloses a system wherein smart cards and remote servers communicate through a host terminal by passing network packets from the smart card and the server that contain smart card commands instructions (i.e. APDUs) (Col. 22, line 51-

Col. 23, line 20), which meets the limitation of translating said requests into APDU format and transmitting said APDU formatted requests to a second server data processing means, second server data processing means for encapsulating said APDU formatted requests received from said first server data processing means into outgoing message packets and transmitting said outgoing message packets over said network to said local client using said server communications means, separating encapsulated APDUs from said incoming message packets thus generating desencapsulated APDUs and routing said desencapsulated APDUs to a fourth server data processing means, and fourth server data processing means for receiving and translating said desencapsulated APDUs sent by said third server data processing means into another message format thus generating a translated message and transmitting said translated message to at least one applications level program. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the secure token access system of DiGiorgio to provide network communication between the secure token device and the ISP server in the manner discussed in the Graham in order to provide multi-application secure token devices that are customizable and allow for unique variations of applications to be loaded onto the individual card post-issuance as taught by Graham (Col. 5, lines 7-18). DiGiorgio does not specify that the APDUs are encapsulated into data packets, and deencapsulated from data packets. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to encapsulate the packets transmitted from the local computer to the remote computer in DiGiorgio using SSL in order to provide a security in communications over networks that is platform independent, that can work with many different types of applications

that request a wide variety of different types of server applications, and which can be performed with minimal time and effort as taught by Elgamal (Col. 1, lines 11-19, 39-55).

Referring to claim 4, DiGiorgio discloses that the network can be the Internet (Col. 1, lines 19-20), which meets the limitation of a public network.

Referring to claim 5, DiGiorgio discloses that the network can be a LAN (Col. 7, lines 28-29), which meets the limitation of a private network.

Referring to claim 6, DiGiorgio discloses that the communications protocol is the Internet Protocol (Col. 1, lines 38-39), which meets the limitation of an open communications protocol.

Referring to claim 7, DiGiorgio discloses that the communications can be encrypted (Col. 11, lines 21-25), which meets the limitation of a secure communications protocol.

Referring to claim 9, DiGiorgio discloses a secure token device access system wherein a secure token device and a local computer system communicate via a token reader, and by passing data packages known as application protocol data units (APDUs) using the reader (Col. 1, line 63 – Col. 2, line 13 & Col. 9, lines 1-6), which meets the limitation of PSD communications means for transmitting and receiving encrypted APDU messages through said PSD interface. When a user attempts to access ISP services from the token device, the ISP issues a challenge to the token device to ensure that the user should be granted access to the ISP services (Col. 2, lines 16-23 & Col. 10, lines 24-33). The computer system utilizes Netscape Navigator, which includes SSL capabilities and would therefore enable two way encrypted communications (Col. 7, lines 44-47), which meets the limitation of first PSD processing means for decrypting incoming encrypted APDU messages using stored cryptographic information, thus generating incoming decrypted APDU messages, second PSD processing means for interpreting said incoming

decrypted APDU messages, and executing commands included in said incoming decrypted APDU messages, third PSD processing means for encrypting outgoing APDU response messages using stored cryptographic information thus generating outgoing encrypted APDU response messages, and transmitting said outgoing encrypted APDU response messages in said APDU format through said PSD interface using said communications means, means for storing at least one cryptographic key. The secure token device contains a unique ID that is encoded into the token device (Col. 10, lines 54-55), which meets the limitation of memory storage means for storing at least one unique identifier.

Referring to claims 10, 15, DiGiorgio discloses a secure token device access system wherein a secure token device and a local computer system communicate via a token reader, and by passing data packages known as application protocol data units (APDUs) using the reader (Col. 1, line 63 – Col. 2, line 13 & Col. 9, lines 1-6), which meets the limitation of server communications means for transmitting and receiving messages over said network using said packet based communications protocol. Once the challenge is received at the token device, the token device issues a response to the ISP challenge in the form shown in Figure 8B (Col. 10, lines 33-35). The computer system utilizes Netscape Navigator, which includes SSL capabilities and would therefore enable two way encrypted communications (Col. 7, lines 44-47), which meets the limitation of cryptography data processing means, first server data processing means fro receiving requests from at least one applications level program. DiGiorgio does not specify that the ISP services provide command instructions to the secure token device and visa versa. Graham discloses a system wherein smart cards and remote servers communicate through a host terminal by passing network packets from the smart card and the server that contain smart card

commands instructions (i.e. APDUs) (Col. 22, line 51- Col. 23, line 20), which meets the limitation of translating said requests into APDU format and transmitting said APDU formatted requests to said cryptography data processing means, second server data processing means for encapsulating encrypted APDU formatted requests received from said cryptography data processing means into outgoing message packets transmitting said outgoing message packets over said network using said server communications means, third server data processing means for receiving incoming message packets using said server communications means and separating encapsulated APDUs from said incoming message packets thus generating desencapsulated APDUs and routing said desencapsulated APDUs to said cryptography data processing means, fourth server data processing means for receiving and translating decrypted desencapsulated APDUs send by said cryptography processing means into another message format thus generating a translated message and transmitting said translated message to at least one applications level program, wherein said cryptography data processing means comprises means for encrypting said APDU formatted requests received from said first server data processing means and sending said encrypted APDU formatted requests to said second server data processing means and for decrypting said desencapsulated APDUs received from said third server data processing means and sending said decrypted desencapsulated APDUs to said fourth server data processing means. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the secure token access system of DiGiorgio to provide network communication between the secure token device and the ISP server in the manner discussed in the Graham in order to provide multi-application secure token devices that are customizable and allow for unique variations of applications to be loaded onto the individual card post-issuance as

taught by Graham (Col. 5, lines 7-18). DiGiorgio does not specify that the APDUs are encapsulated into data packets, and deencapsulated from data packets. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to encapsulate the packets transmitted from the local computer to the remote computer in DiGiorgio using SSL in order to provide a security in communications over networks that is platform independent, that can work with many different types of applications that request a wide variety of different types of server applications, and which can be performed with minimal time and effort as taught by Elgamal (Col. 1, lines 11-19, 39-55).

Referring to claims 16, 17, 19, DiGiorgio discloses that the network can be a cellular network (Col. 5, line 39), which meets the limitation of a digital cellular network and a wireless network.

Referring to claims 20, 28, 37, DiGiorgio discloses a secure token device access system wherein a secure token device and a local computer system communicate via a token reader, and by passing data packages known as application protocol data units (APDUs) using the reader (Col. 1, line 63 – Col. 2, line 13 & Col. 9, lines 1-6), which meets the limitation of generating a request to access said PSD on said remote computer system, wherein said request is in a non-native protocol for communicating with said PSD and said request is generated by an API level program. When a user attempts to access ISP services from the token device, the ISP issues a challenge to the token device to ensure that the user should be granted access to the ISP services (Col. 2, lines 16-23 & Col. 10, lines 24-33). Once the challenge is received at the token device, the token device issues a response to the ISP challenge in the form shown in Figure 8B (Col. 10, lines 33-35), which meets the limitation of receiving by said client said request message sent

over said network. DiGiorgio does not specify that the ISP services provide command instructions to the secure token device and visa versa. Graham discloses a system wherein smart cards and remote servers communicate through a host terminal by passing network packets from the smart card and the server that contain smart card commands instructions (i.e. APDUs) (Col. 22, line 51- Col. 23, line 20), which meets the limitation of converting on said remote computer system said request from said non-native protocol into an APDU format request message using a first server data processing means, said remote computer system said APDU format request message into said packet based communications protocol producing an encapsulated request message, using a second server data processing means, transmitting said request message over said network using said packet based communications protocol, processing said request message using a first data processing means to separate said APDU format request message from said request message, routing on said client said APDU format request message through a hardware device port assigned to a PSD interface independently of the origin and integrity of said encapsulated request message, wherein said PSD interface is in processing communication with said PSD, receiving by said PSD said APDU format request message through said PSD interface and processing said APDU format response message into said packet based communications protocol producing an response message, using a second data processing means, transmitting said response message over said network using said packet based communications protocol, receiving said response message sent over said network by said remote computer system, processing said response message using a third server data processing means to separate said APDU response message from said response message thus generating a APDU response message, converting by said remote computer system said APDU response message into a

response in a non-native protocol using a fourth server data processing means and forwarding said response to at least one API level program. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the secure token access system of DiGiorgio to provide network communication between the secure token device and the ISP server in the manner discussed in the Graham in order to provide multi-application secure token devices that are customizable and allow for unique variations of applications to be loaded onto the individual card post-issuance as taught by Graham (Col. 5, lines 7-18). DiGiorgio does not specify that the APDUs are encapsulated into data packets, and deencapsulated from data packets. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to encapsulate the packets transmitted from the local computer to the remote computer in DiGiorgio using SSL in order to provide a security in communications over networks that is platform independent, that can work with many different types of applications that request a wide variety of different types of server applications, and which can be performed with minimal time and effort as taught by Elgamal (Col. 1, lines 11-19, 39-55).

Referring to claim 21, DiGiorgio discloses that the network can be the Internet (Col. 1, lines 19-20), which meets the limitation of a public network.

Referring to claim 22, DiGiorgio discloses that the network can be a LAN (Col. 7, lines 28-29), which meets the limitation of a private network.

Referring to claim 23, DiGiorgio discloses that the communications protocol is the Internet Protocol (Col. 1, lines 38-39), which meets the limitation of an open communications protocol.

Referring to claim 24, DiGiorgio discloses that the communications can be encrypted (Col. 11, lines 21-25), which meets the limitation of a secure communications protocol.

Referring to claim 25, DiGiorgio discloses that system may automatically attempt to grant the user access to the ISP services once the token device is authenticated (Col. 10, lines 24-28), which meets the limitation of said communication pipe is initiated automatically upon connection of said PSD to said local client.

Referring to claims 26, 27, DiGiorgio discloses that the access to the ISP services may be granted upon a user double click on an icon associated with the ISP (Col. 10, lines 24-26), which meets the limitation of said communications pipe is initiated by a client requesting access to information contained on one or more networked clients or networked remote computer systems.

Referring to claims 29, 36, 37, DiGiorgio discloses a secure token device access system wherein a secure token device and a local computer system communicate via a token reader, and by passing data packages known as application protocol data units (APDUs) using the reader (Col. 1, line 63 – Col. 2, line 13 & Col. 9, lines 1-6), which meets the limitation of generating a request to access said PSD on said remote computer system, wherein said request is in a non-native protocol for communicating with said PSD and said request is generated by an API level program. When a user attempts to access ISP services from the token device, the ISP issues a challenge to the token device to ensure that the user should be granted access to the ISP services (Col. 2, lines 16-23 & Col. 10, lines 24-33). The computer system utilizes Netscape Navigator, which includes SSL capabilities and would therefore enable two way encrypted communications (Col. 7, lines 44-47). Once the challenge is received at the token device, the token device issues a response to the ISP challenge in the form shown in Figure 8B (Col. 10, lines 33-35). DiGiorgio

does not specify that the ISP services provide command instructions to the secure token device and visa versa. Graham discloses a system wherein smart cards and remote servers communicate through a host terminal by passing network packets from the smart card and the server that contain smart card commands instructions (i.e. APDUs) (Col. 22, line 51- Col. 23, line 20), which meets the limitation of converting on said remote computer system said request from said non-native protocol into an APDU format request message using a first server data processing means, and sending said APDU format request message to a cryptography data processing means, receiving and encrypting said APDU format request message using cryptography data processing means thus generating an encrypted APDU request message and sending said encrypted APDU request message to a second server data processing means, wherein said cryptography data processing means uses a pre-established encryption method, on said remote computer system said encrypted APDU request message into said packet based communications protocol producing an and encrypted request message, using said second server data processing means, transmitting said and encrypted request message over said network using said packet based communications protocol, receiving said encapsulated and encrypted request message sent over said network by said client, processing said and encrypted request message using a first client data processing means to separate said encrypted APDU request message from said and encrypted request message thus generating a encrypted APDU request message, routing on said client said encrypted APDU request message through a hardware device port assigned to a PSD interface independently of the origin and integrity of said and encrypted request message, wherein said PSD interface is in processing communication with said PSD, receiving said encrypted APDU request message through said PSD interface by said PSD and decrypting said

encrypted APDU request message using an internal PSD data cryptography means thus generating a and decrypted APDU request message, wherein said cryptography means is pre-established and sending said and decrypted APDU request messages to a first internal PSD data processing means, receiving said and decrypted APDU request message from said internal PSD data cryptography means and processing said desencapsulated and decrypted APDU request message using said first internal PSD data processing means, generating a response message in APDU format by said PSD using a second internal PSD data processing means, encrypting said APDU format response message using said internal PSD data cryptography means thus generating an encrypted APDU format response message response message through said PSD interface, and transmitting said encrypted APDU format receiving by said client said encrypted APDU format response message through said PSD Interface and said encrypted APDU format response message into said packet based communications protocol producing an and encrypted response message, using a second client data processing means, transmitting said message over said network using and encrypted response said packet based communications protocol, receiving by said remote computer system said and encrypted response message sent over said network, processing said and encrypted response message using a third server data processing means to separate said encrypted APDU response message from said and encrypted response message thus generating a encrypted APDU response message, decrypting said encrypted APDU response server data processing means message received from said third using said cryptography data processing means thus generating a and decrypted APDU response message and sending said and decrypted APDU response message to said fourth server data processing means, and converting by said remote computer system said and decrypted APDU response

message into a response in a non-native protocol using a fourth server data processing means, and forwarding said response to at least one API Level Program. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the secure token access system of DiGiorgio to provide network communication between the secure token device and the ISP server in the manner discussed in the Graham in order to provide multi-application secure token devices that are customizable and allow for unique variations of applications to be loaded onto the individual card post-issuance as taught by Graham (Col. 5, lines 7-18). DiGiorgio does not specify that the APDUs are encapsulated into data packets, and deencapsulated from data packets. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to encapsulate the packets transmitted from the local computer to the remote computer in DiGiorgio using SSL in order to provide a security in communications over networks that is platform independent, that can work with many different types of applications that request a wide variety of different types of server applications, and which can be performed with minimal time and effort as taught by Elgamal (Col. 1, lines 11-19, 39-55).

Referring to claim 30, DiGiorgio discloses that the network can be the Internet (Col. 1, lines 19-20), which meets the limitation of a public network.

Referring to claim 31, DiGiorgio discloses that the network can be a LAN (Col. 7, lines 28-29), which meets the limitation of a private network.

Referring to claim 32, DiGiorgio discloses that the communications protocol is the Internet Protocol (Col. 1, lines 38-39), which meets the limitation of an open communications protocol.

Referring to claim 33, DiGiorgio discloses that the communications can be encrypted (Col. 11, lines 21-25), which meets the limitation of a secure communications protocol.

Referring to claims 34, 35, DiGiorgio discloses that the access to the ISP services may be granted upon a user double click on an icon associated with the ISP (Col. 10, lines 24-26), which meets the limitation of said communications pipe is initiated by a client requesting access to information contained on one or more networked clients or networked remote computer systems.

Referring to claims 38, 39, 41, DiGiorgio discloses that the network can be a cellular network (Col. 5, line 39), which meets the limitation of a digital cellular network and a wireless network.

6. Claims 18, 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over over DiGiorgio, U.S. Patent No. 6,385,729, in view of Graham, U.S. Patent No. 6,402,028, in view of Elgamal, U.S. Patent No. 5,657,390 as applied to claims 1, 20 above, and further in view of Brown, U.S. Patent No. 5,455,863. Referring to claims 18, 40, DiGiorgio does not disclose that the network can be optical. Brown discloses a network authentication system wherein the network is wireline, optical fiber link, satellite, or any other type of communication channel (Col. 8, lines 56-58). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the network of Chan to be optical because Brown discloses that those skilled in the art would understand that different networks can be used without departing from the spirit and scope of the invention (Col. 8, lines 48-55).

Double Patenting

7. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or

improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

8. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

9. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

10. Claims 1-4, 7-10, 13-15 of Patent No. 7,363,486 contain(s) every element of claims 1-7, 9, 10, 15-42 of the instant application and as such are not patentably distinct from an earlier patent claim(s).

11. Claims 1-11, 13, 15-16 of Patent No. 7,162,631 contain(s) every element of claims 1-7, 9, 10, 15-42 of the instant application and as such are not patentably distinct from an earlier patent claim(s).

"A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or anticipated by, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140 F.3d at 1437, 46

USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus)." ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

"Claim 12 and Claim 13 are generic to the species of invention covered by claim 3 of the patent. Thus, the generic invention is "anticipated" by the species of the patented invention. Cf., Titanium Metals Corp. v. Banner, 778 F.2d 775, 227 USPQ 773 (Fed. Cir. 1985) (holding that an earlier species disclosure in the prior art defeats any generic claim). This court's predecessor has held that, without a terminal disclaimer, the species claims preclude issuance of the generic application. In re Van Ornum, 686 F.2d 937, 944, 214 USPQ 761, 767 (CCPA 1982); Schneller, 397 F.2d at 354. Accordingly, absent a terminal disclaimer, claims 12 and 13 were properly rejected under the doctrine of obviousness-type double patenting" (In re Goodman (CA FC) 29 USPQ2d 2010 (12/3/1993).

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN E. LANIER whose telephone number is (571)272-3805. The examiner can normally be reached on M-Th 6:00am-4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132